

PHNL031122

PCT/IB2004/051650

11

## CLAIMS:

1. A method of receiving a broadcast signal, the method comprising the steps of
  - receiving an encoded broadcast signal (100) in a receiver (200) from a broadcast device (300), where the encoded broadcast signal (100) have been encoded on the basis of at least one region code (RC1, RC2, ...) each representing a region,
  - 5 - obtaining a region code (RC1, RC2, ...) of a region that the receiver (200) is located in,
  - obtaining a decoding key ( $D_k$ ) in the receiver (200), and
  - decoding the broadcast signal (100) using the obtained decoding key ( $D_k$ ) and on the basis of the obtained region code (RC1, RC2, ...).
- 10 2. A method according to claim 1, characterized in that the method further comprises the step of obtaining a pay-mode (PM1, PM2, ...) and in that the step of decoding the broadcast signal (100) further comprises using a pay-mode key ( $PM_k$ ) being dependent on the obtained pay-mode (PM1, PM2, ...).
- 15 3. A method according to claim 2, characterized in that
  - the decryption key ( $D_k$ ) is derived on the basis of the obtained region code (RC1, RC2, ...) and the pay-mode key ( $PM_k$ ) is independent of the obtained region code (RC1, RC2, ...), or
  - 20 - the pay-mode key ( $PM_k$ ) is derived on the basis of the obtained region code (RC1, RC2, ...) and the decryption key ( $D_k$ ) is independent of the obtained region code (RC1, RC2, ...), or
  - the decryption-key ( $D_k$ ) and the pay-mode key ( $PM_k$ ) are derived on the basis of the obtained region code (RC1, RC2, ...).
- 25 4. A method according to claim 2, characterized in that the pay-mode (PM) is derived on the basis of the obtained region code (RC1, RC2, ...).

PHNL031122

PCT/IB2004/051650

12

5. A method according to claim 1, characterized in that the step of obtaining a region code (RC1, RC2, ...) of a region that the receiver (200) is located in comprises:

- obtaining Global Positioning System (GPS) data from location determination means (206) and using the obtained GPS data to derive the region code (RC1, RC2, ...).

5

6. A method according to claim 1, characterized in that the method further comprises the step of:

- presenting to a user of the receiver (200) an amount to be paid in order to be presented with the broadcast signal (100) and presenting the broadcast signal (100) only if the user accept a payment of the amount.

10

7. A method according to claim 1, characterized in that the step of obtaining a decoding key ( $D_k$ ) comprises:

- selecting a secure cryptographic key and obtaining the decoding key ( $D_k$ ) by performing a function on the secure cryptographic key and the obtained region code (RC1, RC2, ...).

15

8. A method according to claim 2, characterized in that the step of obtaining a pay-mode key ( $PM_k$ ) comprises:

- selecting a secure cryptographic key and obtaining the pay-mode key ( $PM_k$ ) by performing a function on the secure cryptographic key and the obtained region code (RC1, RC2, ...).

20

9. A method of transmitting a broadcasting signal, the method comprising the steps of:

25

- obtaining, in a broadcast device (300), a signal (S) to be transmitted to a number of receivers (200),
- encoding the signal (S) with a number of orthogonal encoding keys ( $E_{k,1}, E_{k,2}, E_{k,3}, \dots$ ) and on the basis of one or more a region codes (RC1, RC2, ...) representing a region, thereby generating an encoded broadcast signal (100), and
- transmitting the encoded broadcast signal (100) to a number of receivers (200).

30

10. A method according to claim 9, characterized in that the method further comprises the step of:

- encoding the signal (S) or the encoded broadcast signal (100) with at least one pay-mode (PM) or pay-mode key ( $PM_k$ ) prior to transmitting the encoded broadcast signal (100).
- 5 11. A method according to claim 10, characterized in that
- the encoding keys ( $E_{k,1}, E_{k,2}, E_{k,3}, \dots$ ) is dependent on the one or more region codes (RC1, RC2, ...) and the pay-mode key ( $PM_k$ ) is independent of the one or more region codes (RC1, RC2, ...), or
  - the pay-mode key ( $PM_k$ ) is dependent on the one or more region codes (RC1, RC2, ...), and the encoding keys ( $E_{k,1}, E_{k,2}, E_{k,3}, \dots$ ) are independent of the one or more region codes (RC1, RC2, ...), or
  - the encoding keys ( $E_{k,1}, E_{k,2}, E_{k,3}, \dots$ ) and the pay-mode key ( $PM_k$ ) are dependent on the obtained region codes (RC1, RC2, ...).
- 10
- 15 12. A broadcast device (300) comprising
- an encoder (302) for receiving a signal (S) to be transmitted to a number of receivers (200) and for encoding the signal (S) with a number of orthogonal encoding keys ( $E_{k,1}, E_{k,2}, E_{k,3}, \dots$ ) and on the basis of one or more a region codes (RC1, RC2, ...), thereby generating an encoded broadcast signal (100), and
  - a transmitter circuit (301) for transmitting the encoded broadcast signal (100) to a number of receivers (200).
- 20
13. A receiver device (200) comprising
- a receiver circuit (201) for receiving an encoded broadcast signal (100) from a broadcast device (300), where the encoded broadcast signal (100) have been encoded on the basis of at least one region code (RC1, RC2, ...) each representing a region,
  - location determination means (202, 206) for obtaining a region code (RC1, RC2, ...) of a region that the receiver (200) is located in,
  - means (202) for obtaining a decoding key ( $D_k$ ), and
  - a decoder (202) for decoding the broadcast signal (100) using the obtained decoding key ( $D_k$ ) and on the basis of the obtained region code (RC1, RC2, ...).
- 25
- 30
14. A broadcasting system comprising at least one broadcast device (300) according to claim 12 and at least one receiver device (200) according to claim 13.

15. A computer readable medium having stored thereon instructions for causing one or more processing units to execute the method according to any one of claims 1 – 8 or to execute the method according any one of claims 9 – 11.